SUMMARY OF THE
INTERIM APPROVAL TO OPERATE (IATO) PROCESS

1.0 Background

An Interim Approval To Operate (IATO) is conducted to ascertain the extent to which an application, system or network meets the Department of Defense (DoD) C2 and Military Health System (MHS) Information Assurance (IA) security requirements. The requirements are set forth in DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria," dated December 1985 and in the "MHS Information Assurance Policy Manual (Draft)," November 2001.

The steps in the IATO process are:

a. The MHS IA C&A Team and the Contractor participate jointly in a kick-off meeting designed to finalize an agreed to timeline to accomplish all necessary actions to complete the IATO. A model timeline is provided, see Attachment 1.

b. The Contractor assists the MHS IA Certification and Accreditation (C&A) Team with the development of a draft System Security Authorization Agreement (SSAA). A template for an SSAA is provided, see Attachment 3.

c. The Contractor assists the MHS IA C&A Team with the development of a draft Security Design Document (SDD). An SDD template is provided, see Attachment 2.

d. The Contractor prepares for and supports an on-site C2 and Minimum Security Requirements test conducted by an MHS IA Analyst. The checklist for this testing is provided to the Contractor prior to the test.

e. The MHS IA C&A Team provides a list of identified vulnerabilities to the contractor upon completion of the C2 and Minimum Security Requirements testing.

f. Vulnerabilities discovered during the C2 and Minimum Security Requirements testing are mitigated by the contractor.

g. Once the contractor mitigates vulnerabilities, the MHS IA C&A Team performs an on-site mitigation validation of previously identified vulnerabilities.

h. The MHS IA C&A Team prepares an IATO Report (risk assessment) with a recommendation on whether to grant the IATO. A sample report is provided, see Attachment 4.

i. Upon receipt of the IATO report, the Designated Approving Authority (DAA) or DAA Representative (DAAR) determines whether to grant an IATO not to exceed (NTE) a 12-month period.

2.0 Objectives

The objectives of the security evaluation are:

a. Ensure applications, systems and networks are certified and accredited in compliance with DoD 5200.28-STD, Department of Defense Standard – Trusted Computer System Evaluation Criteria and DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

b. Ensure applications, systems and networks adhere to the Information Assurance guidance and requirements in DoD Directive 5200.28, Security Requirements for Automated Information Systems.

c. Ensure system owners and project managers are adhering to the technical requirements contained in DoD and MHS Information Assurance policy and guidance documents.

d. Ensure that DoD, MHS Sensitive but Unclassified (SBU), and Patient Identifiable Data (PID) is protected in compliance with the Privacy Act of 1976 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

3.0 IATO Kick-Off Meeting

The Contractor attends a kick-off meeting and provides the following:

a. Points of contact for completing the IATO.
b. A general overview of the system/network to include general architecture and topology.
c. The Contractor assists the MHS IA C&A Team in jointly developing an IATO timeline mutually acceptable to the MHS and the Contractor, and
d. Participates with the MHS IA C&A Team in establishing roles and responsibilities.

At the kick-off meeting, the MHS IA C&A Team provides an overview of the DITSCAP and additional DITSCAP documentation templates, if required.

4.0 Prepare System Security Authorization Agreement

The Contractor assists the MHS IA C&A Team with the development of a draft SSAA using the format and content requirements provided by the MHS IA C&A Team. The MHS IA C&A Team evaluates the acceptability of the SSAA, and provides comments and recommendations as appropriate. The Contractor is required to correct any deficiencies that the government determines are necessary to mitigate prior to issuance of IATO. SSAA Appendices are not required to support the IATO process; however, they are required to complete the ATO process.

5.0 Prepare Security Design Document

The Contractor assists the MHS IA C&A Team with the development of a draft SDD using the format and content requirements provided by the MHS IA C&A Team. The MHS IA C&A Team evaluates the acceptability of the SDD, and provides comments and recommendations as

appropriate. The Contractor is required to correct any deficiencies that the government determines are necessary to mitigate prior to issuance of IATO.

6.0 Support MHS IA C&A Team Testing

During the IATO process, the MHS IA C&A Team conducts C2 and Minimum Security Requirements testing at the Contractor Site. The test plan is provided to the Contractor to assist in preparing for the test. When the testing is completed, a list of vulnerabilities is provided to the Contractor. The Contractor takes necessary action to mitigate the vulnerabilities in a timely manner. When mitigation activities are complete, the Contractor advises the MHS. Once the Contractor mitigates vulnerabilities, the MHS IA C&A Team performs an on-site mitigation validation of previously identified vulnerabilities.

7.0 IATO Risk Assessment Report

The MHS IA C&A Team prepares a report, documenting the IATO activities and findings which include a recommendation to grant the IATO.

AUTOMATED DATA PROCESSING/INFORMATION TECHNOLOGY (ADP/IT) REQUIREMENTS

1.0 ADP Requirements

The Military Health System (MHS) Information Assurance (IA) Program Office, in compliance with DoD 5200.2-R - Personnel Security Program, 1987, requires all contractors who manage, design, develop, operate or access DoD Automated Information System (AIS) or network to undergo an appropriate background investigation and security awareness training before access is granted to an AIS or network. The only exception is when a contractor owned, contractor operated AIS/network does not have connectivity with a DoD AIS or network. In this case, background investigations for contractor personnel are not required and other safeguards may be used, such as, non-disclosure agreements and documentation of security awareness training. For all other personnel, a level of trustworthiness must be established before granting access to MHS SBU information. Therefore, the contractor must:

- Initiate, maintain, and document minimum personnel security investigations appropriate to the individual's responsibilities and access to MHS SBU information.

- Immediately report to the appropriate government representative if any contractor employee filling a sensitive receives an unfavorable National Agency Check (NAC) adjudication, or if information that would result in an unfavorable NAC becomes known,

- Immediately deny access to any AIS, network or SBU information to any contractor employee if, at any time, the individual receives an unfavorable NAC adjudication, or if directed to do so by the appropriate government representative for security reasons.

- Ensure all contractor personnel receive IA training before being granted access to DoD systems/networks, and/or MHS SBU data.

All contractor personnel must be designated as ADP-I, ADP-II, or ADP-III where their duties meet the criteria of these position sensitivity designations as described in Appendix K, DoD 5200.2-R. Investigations appropriate for position sensitivity designations are (see Paragraph 3-614, DoD 5200.2-R).

ADP I	Background Investigation (BI)
ADP II	DoD National Agency Check Plus Written Inquiries (DNACI) or National Agency Check Plus Written Inquiries (NACI)

ADP III National Agency Check (NAC) or Entrance National Agency Check (ENTNAC).

1.1 ADP Positions Categories

In establishing the categories of positions, other factors may affect the determination, permitting placement in higher or lower categories based on the agency's judgment as to the unique characteristics of the system or the safeguards protecting the system. A level of trustworthiness must be established before granting personnel access to MHS SBU information and AISs and networks with DoD connectivity, to include:

- ADP-1 Critical Sensitive Position. Those positions in which the individual is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

- ADP-II Noncritical-Sensitive Position. Those positions in which the individual is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to insure the integrity of the system.

- ADP-III Nonsensitive Position. All other positions involved in computer activities.

Each contractor shall be required to complete and submit the Standard Form 85-P, "Questionnaire for Public Trust Positions," fingerprint forms, and such other documentation as may be required by the Office of Personnel Management (OPM) to open and complete investigations. Forms and guidance can be found at www.opm.gov/extra/investigate

1.2 Non-U.S. Citizens

Non-U.S. citizen contractor employees shall not be assigned to ADP-I positions.

Non-U.S. citizen contractor employees assigned to ADP-II or ADP-III positions must have a completed investigation and favorable adjudication prior to access.

Interim access is not authorized.

Attachment 1 - IATO Timeline

An IATO is granted by the appropriate Designated Approving Authority (DAA) or DAA Representative (DAAR). An IATO is granted for a limited period of time, NTE one year. Below is a summary of the step-by-step process used to support the IATO process.

	IATO Activity	Start Date	Date Due
IATO Activities Timeline			
1	Kick OFF (DITSCAP IATO)		
2	MHS IA C&A Team and the Contractor develop DITSCAP IATO documentation		
	Draft Core SSAA		
	Draft Security Design Document		
3	Security Team review draft IATO documentation		
4	MHS IA C&A Team Develop Security Test Plan and submit to MHS for approval		
5	MHS IA C&A Team review and approve security Test Plan		
6	MHS IA C&A Team perform C2 security testing		
7	Contractor apply any necessary mitigations		
8	MHS IA C&A Team develop and submit vulnerability matrix to the Contractor for review (Identify any vulnerabilities that must be mitigated prior to IATO)		
9	CA review and approve vulnerability matrix and forward matrix to Contractor		
10	Contractor submit vulnerability correction plan of action matrix to the MHS		
11	MHS IA C&A Team validate any Contractor mitigations		
12	MHS IA C&A Team prepare IATO package and submit to CA		

- Automated vulnerability scans may be conducted for an IATO risk assessment to meet special system/network needs when directed by the MHS Certification Authority (CA).